REMARKS/ARGUMENTS

This amendment is presented in response to the Office Action mailed on October 9, 2009. Applicants have included a request for an extension of time extending the time for response to April 09, 2010.

Applicants would first like to express appreciation to the Examiner for review of the Application and remarks. Currently, Claims 7, 8, 10, 11, 14, 20, 22 and 23 are active in the application. Claims 7, 8, 10, 11 14, and 20 have been amended. Claim 22 is currently pending as previously presented and a new dependent Claim 23 has been added. The amendments to the Claims were made to point out with greater particularity the subject matter of the present invention as discussed herein. Claims 12-13, 15-19 and 21 have been canceled without prejudice to eliminate redundancies and / or inconsistencies. For example, Claims 18-19 were canceled because when Claim 7 was amended to clarify the relationship between security levels, this produced redundancies in Claims 18-19. Similar amendments regarding the relationship between security levels were also made to Claim 14.

It should be noted that cancelation of Claims 1-6, that were a direct translation of the claims of an originally filed French priority application, was not done for purposes of limiting the scope of the original claims but rather done to present the claims in better form for examination.

Further, the Examiner is asked to examine all of the above claims as now presented in amended form above with the scope of the claims as now presented, in view of the Specification, and as supported in the Specification.

Comments on Response to Arguments Section of Office Action And Regarding Claim 7

With regards to Claim 7, Claim 7 has been amended to clarify that the client application is running on a client machine linked to a client network, and the client application attempts to establish communication with a server machine linked to a server network in order to exchanges messages with the server application. This is consistent with the description of an illustrated embodiment in Applicants application, that describes the gateway machine as being configured to establish a first and a second connection at a first and a second security level, with the first connection providing a connection from the client machine to the gateway machine, and the second connection providing a connection from the gateway machine to the server machine. Also, as described in an illustrated embodiment, the gateway machine routes messages between the client application on the client machine connected to the client network and the server application on the server machine connected to the server network, and further handles security processing at a first security level for messages being exchanged between the client application and the gateway machine. This processing at a first security level removes (relieves) the server machine and / or server network from the traffic and processing at that first security level, thus removing load from the server machine and the server network. Such support/description may be found for example in portions of Applicants specification cited and discussed herein.

Applicants submit that the amended claims defining the claimed present invention are consistent and supported by the description of one or more illustrated embodiments contained in the Specification, and Applicants

believe that the foregoing comments sufficiently address the comments set forth in pages 2 through 4 of the Office Action relating to the withdrawal of the rejection of the claims under 35 USC 112 paragraph 1 discussed in greater detail herein. Further, Applicants submit that the claims as amended satisfy fully the requirements of 35 USC 112 paragraph 1 for the reasons discussed in this amendment. Applicants will now consider the comments cited in these pages in greater detail.

The Office Action of October 09, 2009 states on page 3 within the first partial paragraph:

> *"the Specification does not support the idea that the request or connection by the client ... is ever established or actually received by the server machine running the server application"*

The Office Action references page 5 lines 19-29 of the Specification that states the following:

> *" **[0050]** Thus, the thread transfers the messages from the network 10 to the network 11 and from the network 11 to the network 10 so that the connection with the first security level is seen in the network 10 as an end-to-end connection between the client machine and the server machine, without the client application's having to be concerned with the intermediate processing in the gateway machine 9.*
>
> ***[0051]** In order to prevent the functionalities of the server application that are normally accessible through the port 1 from being accessed by a non-secure connection in the port 2, a sixth step 44 orders the network layer CR of the machine 9 to delete any message sent to the port 2 that is addressed to the server machine 13. An operating system like LINUX, for example, provides a command known as "ipchains-A input-j DENY", which has as parameters a destination port and a destination network address. By giving these parameters, respectively, the value of the port 2,*

for example 8080, and the network address value AR(13) of the machine 13, the network layer CR of the gateway machine 9 can identify any datagram of a message having in its header the values of the first two parameters, and thus delete this message."

Applicants respectfully point out a further description in the Specification describes the establishment of a connection from the gateway machine to the server machine / server network as follows.

1) Paragraph [0042] in the published application describes the second connection as follows:

"[0042] The advantage of the steps of the method just described is that the first security level is limited to the client network 10. In order to allow the ***server application*** *17* ***to communicate with the client application*** *16* ***using a second security level*** *in the server network 11, a fifth step 41* ***defines a port 2 of the server application*** *17.* ***This port 2 is designed to receive connections with the second security level,*** *through functionalities of the server application that are normally accessible with the first security level. These functionalities are generally distinct from normally accessible functionalities, for example in the port 6."*

This paragraph describes a port being created for the server application on the server machine to communicate at the second security level in the server network. The words "*to allow the server application to communicate with the client application using a second security level*" seem clearly to mean that the server application is in communication with the client application.

2) Adding to this paragraph, the description in paragraph [0050 states the following:

"the thread transfers the messages from the network 10 to the network 11 ... so that the connection with the first security level is seen in the

network 10 as an end-to-end connection between the client machine and the server machine, without the client application's having to be concerned with the intermediate processing by the gateway machine"

It seems clear from Applicants' specification discussed above that the communication between the client and server passes through the gateway machine, with intermediate processing being performed by the gateway machine. The processing by the gateway machine MAY not be visible to the client application, but it does take place and enables the communication between the client application and the server.

3) Figures 1 and 5, and paragraphs [0045] and [0046] in the published application also further describe details of the connections according to an illustrated embodiment(s). Paragraphs [0045] and [0046] are reproduced below for Examiner's convenience, with emphasis added for support of Applicants' argument that there is sufficient support in the Specification describing the server machine sending and receiving messages to and from the client application on the client machine.

*"**[0045]** The connection established in phase 50 is represented in FIG. 5 by a phase 52, which listens to the first interface 56 in order to detect any message entering into it.*

***[0046]** A second phase 51 **establishes a connection with a second security level.** To do this, **a second communication interface to the port 2 of the server machine 13 is opened**. In the case of the LINUX operating system, this interface is known as a "socket." Thus, **each thread has its own second communication interface with the server application 17**. If, for example, the second security level is zero, the connection occurs in a conventional way, as in any non-secure connection."*

A connection may not necessarily be made directly to the server machine from the client machine, but a connection from the gateway machine to the server machine IS established and this is the second connection defined in presently amended Claim 7.

It should be noted that the above paragraphs describe one illustrated embodiment of the present invention, and are included to illustrate support but are not intended to imply a general limitation relating to how threads or processes in the gateway machine might be designed for practicing the claimed invention.

The Office Action further states on page 3 in the second paragraph (first full paragraph) that:

> "*The examiner finds no description in the instant specification that describes the first and second connections (with different security levels) as both being connections to the server machine.*"

Claim 7 as now amended clarifies the characterization of the first and second connections consistent with the above description of the illustrated embodiment by specifying the first connection being established between the client application on the client machine connected to the client network AND the gateway machine and with the second connection being established between the gateway machine and the server machine. Additionally, amended Claim 7 clarifies the differences in security levels according to the teachings of the present invention as viewed with regards to the Specification, and as supported in the Specification.

Claim Rejections - 35 USC § 103

Applicants traverse the rejection of Claims 7-8, 10-12, 14 and 18-22 under 35 U.S.C. 103(a) as being unpatentable over Ilnicki (6751677) in view of Rees (6981265) as applicable to the currently active claims.

With regard to Obviousness, the MPEP notes *"A claimed invention is unpatentable if the differences between it and the prior art are "such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art."* 35 U.S.C. § 103(a) (2000); KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398,406 (2007); Graham v. John Deere Co., 383 U.S. 1, 13-14 (1966).

See also Reference: BPAI Appeal 2009-003923 in Ex parte Kenneth J. Susnjara - Application 09/872,335 decided on July 20, 2009

" In Graham, the Court held that the obviousness analysis is bottomed on several basic factual inquiries: "[(1)] the scope and content of the prior art are to be determined; [(2)] differences between the prior art and the claims at issue are to be ascertained; and [(3)] the level of ordinary skill in the pertinent art resolved." 383 U.S. at 17. See also KSR, 550 U.S. at 406. "The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." Id. at 416. "

With regards to the teachings of Ilnicki, Applicants submit that the Ilnicki reference does not teach or suggest the claimed invention. Recognizing that while the purpose of the Ilnicki invention is not generally used as the basis for argument, it is still useful to compare the purpose of the method taught by Ilnicki with the improvements provided by utilizing one or more improvements or aspects of Applicants' claimed invention as described in Applicants' specification, and to discuss what is taught and claimed by Ilnicki. Ilnicki is directed to the following:

1) [from Ilnicki Claim 1] "*allowing a secure and transparent communication between a user device and servers ... via a firewall AND a gateway ...".*

2) [from Ilnicki Claim 6] "*In a data access network system having servers, a client access device, a firewall, AND a first and second gateway ... a method allowing secure connection ...*"

3) [from Ilnicki Claim 5 and the same language in Claim 10] *"establishing a single SSL (Secure Socket Layer) connection between the user device and the target server."*

4) [from Ilnicki "Field of the Invention"] *"... this invention relates to providing a secure and transparent network gateway that does not require complex configuration to the associated firewall".*

5) [from Ilnicki Column 2, lines 46-65 and Column 3 lines 2-3] (This is in discussion by Ilnicki of the prior art, and the **disadvantages** of the prior art overcome by his invention) *" One disadvantage associated is that the gateway typically does not allow the firewall to provide end to end security .. (e.g. authentication, confidentiality, and integrity) ...*

... This means that a single SSL session cannot be established between the user terminal and the target object servers. ...

... This means that the target object server must be modified to manage user credentials."

6) [Ilnicki Column 8, lines 46-67] (This is in discussion by Ilnicki of the **advantages** of his invention) *"... If the target server is not authenticated, the gateway may try to establish a SSL session WITH THE TARGET SERVER ...*

*... Therefore the gateway will allow AN END TO END **SSL** SESSION between the user terminal and the target server of the servers to be established"*

From the above, it is seen that Ilnicki teaches the following:

- a method of avoiding complex configuration of a gateway and an associated firewall [column 1, lines 14-15];

- an improvement in firewall flexibility [column 1, line 60]; and

- improvements to provide "**end to end security**", and allowing for use of SSL **from end to end** [column 2, lines 4-50].

"SSL" (Secure Sockets Layer) is a protocol developed for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data, a public key and a private key.

Ilnicki should be viewed as teaching away from providing a method of reducing processing in accordance with Applicants' present invention because Ilnicki specifically requires and indeed counts as a goal of his invention, the maintenance of a single level of security from "end to end" and which is not in any way concerned with allowing for any reduction in processing on the servers included therein.

Thus, Ilnicki is teaching a simplification and flexibility of configuration not a method of improving performance, and the practice of Ilnicki's teachings indeed would make it impossible for a skilled artisan to utilize Applicants' invention to perform as intended or be utilized .

Further, Ilnicki is describing improvements for a system that includes or requires the use of a firewall, whereas Applicants' present invention is not concerned with establishing communications through a firewall or firewalls.

As indicated above, Ilnicki does NOT teach, suggest, or is concerned with providing a method of reducing processing by a server application, running on a server machine, or reducing traffic on a server network, which are improvements enabled by practice of at least one embodiment of Applicants' claimed invention as described in the Specification. Additionally, for reasons discussed below, Applicants do not believe that the cited teachings of Rees in combination with Ilnicki overcome this deficiency.

Applicants' claims are directed to providing a gateway machine and offloading security processing from a server, whereas Ilnicki's invention maintains and requires security processing on the server at the same security level as utilized on the client.

With regards to Ilnicki in view of Rees, Rees is cited in the Office Action as teaching a system for relaying messages from an external network into an internal network through a gateway that includes a teaching that messages forwarded to port 1 of a port inside the network can be forwarded to a different port inside the network by the gateway. It is not understood how this teaching is to be applied or combined with the teachings of Ilnicki. The Office Action states that it would have been obvious to one of ordinary skill in the art at the time the invention was made to use Rees teaching of allowing the gateway to redirect a communication from a first port to a second to allow communications external to the target server's network access ports which only internal user's can access.

Applicants claims are not concerned with allowing communications external to a server network access ports which only internal users can access as in the case of a firewall. It is unclear from the stated basis for concluding that the claimed invention is obvious what exactly the grounds for rejection are, that is, are the grounds based on the premise that it is obvious to try to use the cited Rees teaching in Ilnicki? There is no discussion of what would motivate a skilled artisan to attempt to incorporate the cited teaching of Rees into the system of Ilnicki. There is no indication that this combination is seen as a substitution of teachings or functions. Notwithstanding the above, it is clear as well as being evidenced by statements in the Office Action that Rees and Ilnicki whether taken either singularly or in combination DO NOT teach a method directed to connections between a client machine, a gateway and a server machine that enables exchanging messages involving two different security levels as set forth in Applicants' amended claims and interpreted in view of Applicants' Specification and Figures of the Drawing..

Detailed discussion of Rees reference

The cited teachings of Rees will now be considered in greater detail. With regard to the teachings of Rees cited in the Office Action as the basis for rejecting Applicants claims in combination with the teachings of Ilnicki, Applicants submit that there is no suggested reason, need or motivation to attempt to combine the teachings of Rees with Ilnicki in that the teachings of Rees do not solve any problem presented by Ilnicki or suggested in Ilnicki as needing solution. Further, the specific teachings of Rees cited in page 7 of the Office Action do not appear to describe or even suggest any of the claimed elements or steps of Applicants' claimed invention. As stated above, in KSR, "The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." But, Applicants submit that there is nothing in the cited art that indicates that it was predictable to have Ilnicki modified or combined with the teachings of Rees in any way that would give rise to Applicants claimed method which provides two levels of security and reduced server processing.

Applicants will now consider Rees in greater detail. In the Abstract of Rees is found the following description (with emphasis added by underline):

> *"A network gateway (1005) is described,* ***wherein an object invocation (1020) containing an embedded object reference (1025), which points to a further object (1002), is modified on passing*** *through the gateway. The gateway validates the object invocation* ***and enacts a number of security tests thereon*** *before forwarding it on. In preferred embodiments, the embedded object reference is replaced by an object reference (1035) to a gateway proxy specifically for the further object (1002).* ***The replacement object reference (1035) also includes enough information that the original object reference (1025) can be recovered****. The gateway*

proxy is generated on or after receipt of the invocation (1020). In the event the further object (1002), which was the subject of the object reference, is itself invoked, the invocation is directed to the gateway proxy, which in turn recovers the original object reference and forwards the invocation on to the further object (1002)."

In this text above, Rees describes "*object invocation containing an embedded object reference*". The purpose of Rees invention is to control the flow of objects through a gateway proxy. Replacement objects are generated that "*include(s) enough information that the original object reference can be recovered*". This is not equivalent or suggestive of the "security processing" of Applicants' invention. Applicants' invention describes security processing which reduces processing (work) required on a Server machine, achieved by performing that processing (or at least a part of it) on a gateway machine. In contrast, it is clear from Rees that since the replacement object reference of Rees includes enough information that the original object reference can be recovered, that this is not reducing the work (processing) of the server. Rees is merely directing the flow of traffic, and checking the validity of the flow of messages between objects.

In further discussion of security, the following cited text from Rees contained in Col. 3, lines 18-29 relative to Claims 18-19 now applicable to Claim 7, Rees teaches the following:

"The check data preferably comprises the results of a hash operation on at least the identifier, host and port, and a secret. For example, the check data can be used by the gateway to verify that an invocation has arisen from a valid new identifier previously generated by the gateway, rather than from an un-trusted source. Thus, the check data adds a high level of security to the gateway. In this way, even if an un-trusted party

gains knowledge of the location of a valid object on the other side of the gateway, the party will not be able to invoke the object without knowing the hash operation and, more particularly, the secret, which is stored securely by the gateway."

Applicants do not find this description to disclose that Rees teaches a system for providing a trusted gateway between a client and a target server where the communications being received from the gateway are given a higher level of security than any other communications being made across the network as stated in the Office Action. This description in Rees describes a gateway performing verification or checking of an identifier to verify that an invocation is not from an un-trusted source. This process for identifying the trustworthiness of a source can be more properly likened to checking or verifying the degree of privilege or access granted to a source. Accordingly, for this reason and other reasons discussed above, Applicants submit that the statement that the check data adds a high level of security to the gateway is deemed to be in no way indicative that two levels of security processing are involved, as in Applicants' claimed invention. Further, for these reasons and in view of the description of the trusted system of Rees provided herein, Applicants find no reason as to why it would be obvious by one of ordinary skill in the art to allow the gateway in Ilnicki to be considered a trusted gateway allowing the target server to allow the communications from the gateway a higher security level than other connections on the network as stated in pages 7-8 of the Office Action. Moreover, there is no description or suggestion that this check of an identifier saves the server from any work, or reduces traffic on the server network, other than possibly ignoring requests from un-trusted parties.

In normal processing from a trusted source, the processing described by Rees on the gateway would not reduce load on the server or the server network. As previously stated, Rees also does not describe or suggest any changing of security level from one side of a gateway to another. Rees in general is describing a method for validating security in the routing of messages relative to origin of source, and in Rees the "messages" are actually "object" requests with identifiers and not general messages. After careful examination of Rees, Applicants find no suggestion of performing processing in a gateway which reduces load on the server or the server network as discussed above.

Further, Applicants find Rees absent any suggestion of reducing the level of security from the client to the server side of a gateway, and any suggestion of reducing a level of security for purposes of moving processing from the server to the gateway, or for reducing server network traffic.

Thus Applicants submit that in Rees traffic on both sides of the gateway or gateway proxy is at the same level of security, even though validation of requests may occur in the gateway. This is in contrast to Applicants amended claims that according to Applicants teachings enable exchanging messages where the security level is reduced. In Rees, there is a validation check that messages are allowed to be directed as requested, but there is no reduction in the level of security such as for example the level of encryption under which those messages are forwarded or transmitted. In Rees, the savings in processing is on the gateway machine which is described in Rees column 3, lines 62- 67 as follows:

"an appropriate template for an anticipated message as soon as the gateway sees an identifier in a message, the time taken to process an message, which is increased by the gateway needing to generate an

appropriate interface means, or proxy, to process the message, is reduced considerably".

whereas, in illustrated embodiment of Applicants' present invention, the savings is on the server machine, NOT on the gateway machine. In fact, it is not seen how a skilled artisan would consider obvious to combine the teachings of Rees with Ilnicki because Rees is teaching an approach for "checking" validity of message routing, whereas Ilnicki is teaching an approach for securely and flexibly configuring ports of a gateway and a firewall. In view of this, and for the reasons stated above, Applicants further submit that any attempt to combine the teachings of Ilnicki and Rees would yield unpredictable results.

Further, even if combination of Ilnicki and Rees were possible for sake of argument, such combination still would result in neither Rees nor Ilnicki providing a reduction of processing on the server network, a reduction of server network traffic as obtained according to Applicants' teachings or a reduction in the level of security as messages are processed by the gateway.

As discussed above, Claim 7 has been amended to clarify the elements and steps of the claimed invention, and dependent Claims 18 and 19 have been canceled because the limitations of those claims are now redundant in view of the clarifying amendments made to Claim 7.

As previously discussed, as to the cited description of Col. 22, line 50-Col. 23, line 20 in Rees, Applicants find that this description by Rees appears to pertain to the configuration aspects of directly accessible ports on which a trusted relay process (TR) is listening and identification of possible attack strategies and the feature of the configuration that defeats them. It is unclear as to the applicability of these teachings to Applicants claims as

amended. As indicated, Applicants have thoroughly examined the teachings of Rees, and find no further teaching that appears to render obvious Applicants' claimed invention as defined in the current amended claims.

Discussion of REES and CORBA:

Because of the reliance on Rees in the key arguments presented in the Office Action for concluding that Applicants' claimed invention is obvious, Applicants provide for consideration the below descriptive materials taken from Rees and other references to clarify the context and application of Rees' teachings to implementing a trusted proxy or gateway utilized within a secure operating system environment as envisioned by Rees.

As noted above, from Rees [Abstract]: "*the invocation is directed to the gateway proxy, which in turn recovers the original object reference and forwards the invocation on to the further object.*" Rees relates to the handling of objects, not to the handling of messages, and not to the encryption and decryption of messages as an aspect of security processing as described in Applicant's specification by way of example.

From Rees [Col 1, 29-31]: "*how blocks of intelligence, known as objects, interact across a distributed computing and communications environment.*" And from [Col 1, lines 56-57]: "*It is an aim of the present invention* (of Rees) *to provide a gateway which can support CORBA and the like*".

Rees describes CORBA within the section of Background Art of his patent/application [Col 1, lines 28-29] as: "*a model for middleware*

applications" and characterizes CORBA as "*CORBA is a well documented* ... [and not] *considered at any depth in this description".* Serving as prior art however it is important to distinguish between the teachings and standards of CORBA as understood by Rees at the time of that Patent Application, and the messaging system described in Applicants' disclosure.

From Wikipedia, the free online encyclopedia at http://Wikipedia.org CORBA is described as follows::

> *"The Common Object Request Broker Architecture (CORBA) is a standard defined by the* ***Object Management Group****(OMG) that enables software components written in multiple computer languages and running on multiple computers to work together, i.e. it supports multiple platforms. Overview -- CORBA is a mechanism in software for* ***normalizing the method-call semantics between application objects*** *that reside either in the same address space (application) or remote address space (same host, or remote host on a network). Version 1.0 was released in October 1991.* ***CORBA uses an interface definition language*** *(IDL) to* ***specify the interfaces that objects will present to the outside world****. CORBA then specifies a mapping from IDL to a specific implementation language like C++ or Java. Standard mappings exist for Ada, C, C++, Lisp, Ruby, Smalltalk, Java, COBOL, PL/I and Python. There are also non-standard mappings for Perl, Visual Basic, Erlang, and Tcl implemented by object request brokers (ORBs) written for those languages."*

To gain understanding of Rees, at the time of that application, and because CORBA is an evolving standard, Applicants located a document authored by Rees at about the time of the Rees application describing Rees' view of CORBA at that time. A complete copy of that document is attached for the

convenience of the Examiner. The references described below are marked in the attached document.

Ref: HP-1: HP CORBAweb is a software infrastructure that allows access to CORBA applications from the web. HP VirtualVault is a secure environment for web applications.

The paper gives overviews of both VirtualVault and CORBAweb, and describes the **object gateway that merges the integration features of CORBA web with the security of VirtualVault**.

The paper describe **the authorization model that determines the granularity at which access is granted**..

Ref: HP-2: The object gateway is designed to be used **to provide controlled access through a firewall** protecting the servers.

Ref: HP-3: The paper **describes the authorization model that determines the granularity at which access is granted**.

Ref: HP-4: Instead, it runs two web servers, one for the outside network, and one for administration from the inside; and **uses a separate Trusted** Gateway Agent (TGA) to mediate communication between outside and inside.

Ref: HP-5: **CORBA web is a plugin replacement for CGI**: (see figure below)

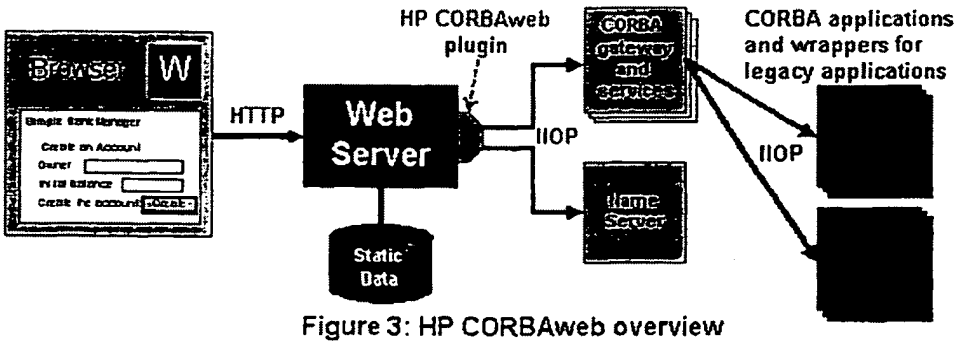

Figure 3: HP CORBAweb overview

How a request is handled

Ref: HP-6: Using CORBA means that we have much choice over placement of the gateway object: it can be on a remote machine, and can be in a dedicated process or share a process with many other gateway objects.

Ref: HP-7: The Secure Object Gateway -- The purpose of the secure object gateway is to give fine grain access control on the services which are accessible from the back-end of the web server. It allows access only to those services which the administrator has authorized explicitly. In addition the administrator can name which users and groups are allowed to access which services

Ref: HP-8: When a service interceptor receives a request for an invocation it checks that the user is authorized to invoke the service.

Ref: HP-9: There are three basic actions which an administrator can apply to the available targets.

1. Verify that the target services still exist by checking that the service is still running and still in the name server
2. Remove the target from the list of available targets
3. Set access controls for the named target

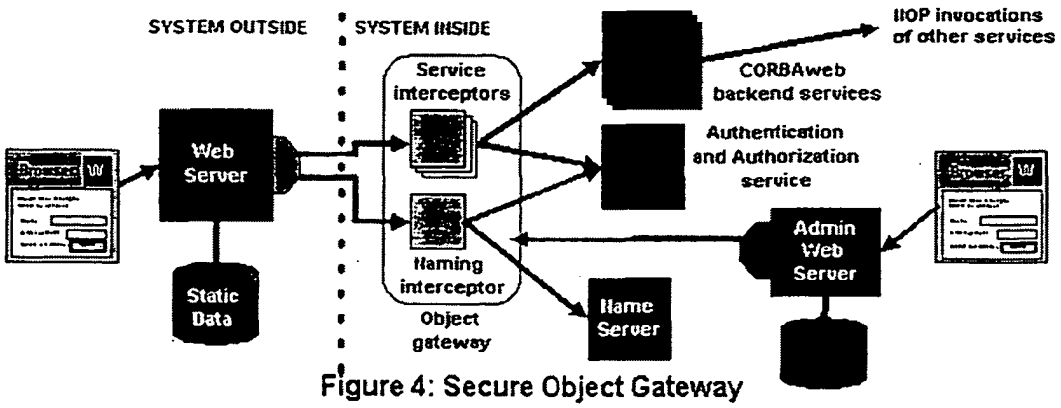

Figure 4: Secure Object Gateway

All of the emphasized description above, describing CORBA, is not at all a part of a conventional client/server network messaging system with the Security Processing (e.g. encryption and decryption) such as the type of system to which Applicants' claims are directed, supported and as interpreted in light of Applicants' Specification.

Based on this dissimilarity of Rees' use of CORBA in comparison with the messaging system described in the illustrated embodiments of Applicants' present invention, Applicants submit that independent Claims 7 and 14 distinguish patentably over such known prior art, including Ilnicki viewed with respect to Rees.

Applicants also submit that presented Claims: 8, 10, 11, 20, 22 and also including newly presently presented Claim 23, as dependent claims, also distinguish patentably over the prior art for the same reasons discussed above with regards to Claims 7 and 14 on which such Claims depend.

Conclusion:

Applicants again thank the Examiner for the review and remarks presented in the Office Action. It is hoped that the amendments to the Claims in view of these remarks now make clear and describe Applicants' present invention.

In view of the above arguments and clarifying amendments, Applicants submit that presently presented Claims 7-8, 10-11, 14, 20-22 and new Claim 23 should be deemed patentable over the currently and previously cited prior art. A notice to this effect is respectfully solicited. Applicants ask the Examiner to contact Applicant's representative to further discuss any grounds for rejecting Applicants claims if necessary before acting on this amendment. Also, if any questions or issues should arise with respect to this amendment or the allowability of this application, the Examiner is urged to call Applicants' representative at the number indicated herein.

Applicants further specify that the preceding arguments and discussion are for purposes of discussing one or more illustrated embodiments of Applicants' invention and should not be construed as limiting. The bounds of the claimed invention are as defined in Applicants' claims as interpreted in light of the specification.

Additionally, if the Examiner feels that further discussion may further advance the prosecution of this application, the Examiner is urged to call the phone number below at any time.

Respectfully submitted,

Russell W. Guenthner Date: March 11, 2010

Russell W. Guenthner, Ph.D. Reg. # 54,140
Bull HN Information Systems Inc.
13430 North Black Canyon Highway
Phoenix, Arizona 85029

Office Phone Number: 602 862-5479